



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada



2010 Methodology for Assessing Disruptions (MAD) Game Part 1

Report and Analysis

Gitanjali Adlakha-Hutcheon, DRDC Corporate
Mark Hazen, DRDC Atlantic
Paul Hubbard, DRDC Ottawa
Scott McLelland, DRDC Ottawa
Kevin Sprague, DRDC Ottawa

Defence R&D Canada – Corporate

Technical Memorandum
DRDC Corporate TM 2012-009
December 2012

Canada

2010 Methodology for Assessing Disruptions (MAD) Game Part I

Report and Analysis

Gitanjali Adlakha-Hutcheon, DRDC Corporate
Mark Hazen, DRDC Atlantic
Paul Hubbard, DRDC Ottawa
Scott McLelland, DRDC Ottawa
Kevin Sprague, DRDC CORA

Defence R&D Canada – Corporate

Technical Memorandum

DRDC Corporate TM 2012-009

December 2010

Principal Author

Original signed by G. Adlakha-Hutcheon, M. Hazen, P. Hubbard, S. McLelland, K. Sprague

G. Adlakha-Hutcheon, M. Hazen, P. Hubbard, S. McLelland, K. Sprague

MAD Games Organizing Team

Approved by

Original signed by Pierre Lavoie

Pierre Lavoie

Chief Scientist, DRDC

Approved for release by

Original signed by Pierre Lavoie

Pierre Lavoie

Chief Scientist, DRDC

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2010

© Sa Majesté la Reine (en droit du Canada), telle que représentée par le ministre de la Défense nationale, 2010

Abstract

The memorandum reports on the Methodology for Assessing Disruptions (MAD) game played at DRDC Ottawa on 5-6 October 2010. This event was Part I of a two-part seminar wargame. In Part I, scientists and CF members participated in a two-step brainstorming and red-teaming process to develop futuristic ideas of systems that may provide an operational advantage to the CF. A total of 47 idea of system cards were produced in Part I. These will be assessed for their disruptive potential through a series of wargames in Part II, which will take place in January, 2011. Feedback solicited through a Judgments and Insights session and formal feedback forms brought to light several ideas for improving the gaming methodology for future iterations of MAD. The game was successful in fostering innovation through confrontation-based red-teaming as well as socializing potentially disruptive technologies elaborated in the ADM (S&T) Functional Planning Guidance. This memorandum is intended primarily for the Office of the Chief Scientist (OCS) DRDC and the Chief Scientists Network (CSNet). It will also be of interest to others in the S&T community within DRDC and its CF partner organizations such as the Chief Force Development and the environmental warfare centres.

Résumé

Le mémorandum technique traite du jeu MAD (méthodologie d'évaluation des perturbations) joué à RDDC Ottawa les 5 et 6 octobre 2010. Cet événement fut la première partie d'un exercice de jeu de guerre en deux composantes. Dans la première partie, des scientifiques et des membres des FC ont participé à un processus en deux étapes de remue-méninges avec équipes rouges dans le but d'élaborer des idées de systèmes futuristes susceptibles de fournir un avantage opérationnel aux FC. Au total, 47 cartes d'idées de systèmes ont été réalisées au cours de la première partie. Celles-ci seront évaluées pour leur potentiel perturbateur dans le cadre d'une série de jeux de guerre lors de la deuxième partie qui aura lieu en janvier 2011. La rétroaction sollicitée par l'entremise d'une séance de jugements et d'idées ainsi que de formulaires de rétroaction formelle ont mis en lumière plusieurs idées permettant d'améliorer la méthodologie des jeux pour les versions futures des jeux MAD. Le jeu a permis de favoriser l'innovation grâce à l'utilisation d'équipes rouges fondée sur la confrontation de même qu'à la socialisation de technologies potentiellement perturbatrices élaborées dans le Guide de planification fonctionnelle du groupe du SMA(S&T). Le présent mémorandum technique est principalement destiné au Bureau du scientifique en chef (BSC) de RDDC et au Réseau des scientifiques en chef (CSNet). Elle pourra également intéresser d'autres intervenants de la collectivité des S & T au sein de RDDC et des organisations partenaires des FC, notamment le Chef du Développement des Forces et les centres de guerres environnementales.

This page intentionally left blank.

Executive summary

Methodology for Assessing Disruptions (MAD) Game Part I: Report and Analysis

Gitanjali Adlakha-Hutcheon, Mark Hazen, Paul Hubbard, Scott McLelland, Kevin Sprague; DRDC Corporate TM [DRDC-TM-2010-012]; Defence R&D Canada – Corporate; December 2010.

Introduction: The ‘Methodology for Assessing Disruptions’ (MAD) game is a combination of structured brainstorming and seminar wargaming that are used as a tool to assess ‘potentially disruptive technologies’ (PDTs) for the ADM(S&T) of DND. The game brings together scientists or innovators from DRDC, and officers or users from the Canadian Forces (CF) to advance insight into futuristic technological systems of military relevance to our forces. The MAD games are a *Canadianized* version of the Disruptive Technology Assessment Game (DTAG) designed by NATO. The MAD games are played in two parts, where Part I is a brainstorming exercise designed to harness the scientific creativity of the DRDC S&T professionals in developing futuristic systems that could provide an operational advantage to our CF partners. Part II of the games test the output of Part I in a seminar wargame setting. Part I was accomplished using structured brainstorming where two Purple teams developed ‘technological solutions’ known as ‘Idea of Systems’ (IoS) cards, within the area of potentially disruptive technologies, to achieve blue force objectives in operational vignettes that are set within an expeditionary scenario developed by Chief of Force Development (CFD). This brainstorming activity was followed by ‘red-teaming’ whereby each Purple team was given the chance to trial their IoS cards against a Red team formed of CF officers within the context of the vignette. This second step was critical for pushing the boundaries of creative thought and testing the IoS cards from an operational point of view.

Results: The MAD Game Part I was played at DRDC Ottawa on October 5 & 6, 2010 and brought together 24 participants from seven DRDC centres and four CF partner organizations, including CFD, Chief of Defence Intelligence (CDI) and two warfare centres. The event achieved its objective of developing IoS cards with participants creating a total of 47 IoS cards covering 7 PDT areas. The two Purple teams, composed of DRDC S&T professionals and a military advisor developed a total of 18 IoS cards. The Red team, comprised of military operators and a scientific advisor, developed 13 IoS cards. All team participants were also invited to develop their own IoS cards independently, yielding an additional 16 new cards.

A second set of results was associated with ways to improve the gaming methodology itself. It was clear that the two-step process used for Part I, i) brainstorming and ii) red-teaming via confrontation was instrumental in fostering innovative ideas. Red-teaming via confrontation with the Red team enabled the identification of vulnerabilities in the cards. A further meta-analysis of MAD Part I revealed that this could be refined by making it a three-step process with the addition of a common session where the Purple and Red teams together strengthen the IoS cards. This alteration in methodology is expected to lead to a robust set of IoS cards, rather than an attempt between the teams to ‘win’ the game.

Significance: The MAD Game Part I succeeded in developing ideas for Horizon II & III systems that exploit PDT. The extent to which these ideas will influence DRDC R&D planning will be known upon conducting Part II. Both the DRDC and CF personnel were actively engaged in the process and felt that it was a worth-while endeavor. Part I also established the usefulness of red-teaming to produce better IoS cards and to socialize the ideas about future technologies among the participants from several DRDC centres.

Future plans: The IoS cards from Part I will be assessed for their disruptive potential in Part II of the MAD games. Part II, which will be held in early 2011, will be a conventional seminar wargame where CF Red and Blue teams develop Courses of Action (COA) to achieve the assigned mission objectives and then are given the IoS cards to determine which cards disrupt a team's COA. The disruptive potential of a card will be determined on the basis of the difference in the COA in the presence and absence of the card. Taken together Part I and II will help to influence the investment decisions associated with the PDT life cycle.

Sommaire

Methodology for Assessing Disruptions (MAD) Game Part I: Report and Analysis

Gitanjali Adlakha-Hutcheon, Mark Hazen, Paul Hubbard, Scott McLelland, Kevin Sprague; DRDC Corporate TM [DRDC-TM-2010-012]; R & D pour la défense Canada – Corporate; Décembre 2010.

Introduction : Le jeu MAD (méthodologie d'évaluation des perturbations) consiste en un remue-ménages structuré et en un exercice de jeu de guerre qui servent d'outil pour évaluer les technologies potentiellement perturbatrices à l'intention du SMA(S & T) du ministère de la Défense nationale (MDN). Le jeu réunit des scientifiques et des novateurs de Recherche et développement pour la défense Canada (RDDC), de même que des officiers ou des utilisateurs des Forces canadiennes (FC) pour obtenir un aperçu des systèmes technologiques futuristes d'intérêt militaire au profit de nos forces. Les jeux MAD se veulent une version *canadienne* du DTAG (jeu pour l'évaluation des technologies perturbatrices) conçu par l'Organisation du Traité de l'Atlantique Nord (OTAN). Les jeux MAD se divisent en deux parties. La première partie comporte un exercice de remue-ménages visant à exploiter la créativité scientifique des professionnels de S & T de RDDC pour ce qui est de l'élaboration de systèmes futuristes susceptibles de procurer un avantage opérationnel à nos partenaires des FC. La deuxième partie des jeux évalue les résultats de la première partie dans le cadre d'un exercice de jeu de guerre. La première partie a été réalisée au moyen d'un remue-ménages structuré où deux équipes « mauves » ont élaboré des solutions technologiques connues sous le nom de cartes Idée de Système (IdS), dans le domaine des technologies potentiellement perturbatrices, afin d'atteindre les objectifs des forces bleues des vignettes opérationnelles établis dans le cadre d'un scénario expéditionnaire conçu par le Chef du Développement des Forces (CDF). Cette activité de remue-ménages a été suivie par la création d'équipes rouges, où chaque équipe mauve avait l'occasion de faire l'essai de leurs cartes IdS contre une équipe rouge composée d'officiers des FC dans le contexte des vignettes. Cette deuxième étape se révélait essentielle pour repousser les limites de la pensée créative et mettre à l'essai les cartes Système d'un point de vue opérationnel.

Résultats : La première partie du jeu MAD a été jouée à RDDC Ottawa les 5 et 6 octobre 2010. Ce jeu a réuni 24 participants issus de sept centres RDDC et quatre organisations partenaires des FC, y compris, le CDF, le Chef du renseignement de la Défense et deux centres de guerres. Cet événement a atteint son objectif, lequel consistait à réaliser des cartes IdS avec les participants. Cela a donné lieu à la création de 47 cartes au total, couvrant sept domaines liés aux technologies potentiellement perturbatrices. Les deux équipes mauves, composées de professionnels de S & T au sein de RDDC et d'un conseiller militaire ont réalisé au total 18 cartes IdS. L'équipe rouge, formée d'opérateurs militaires et d'un conseiller scientifique, a réalisé 13 cartes IdS. Les participants de toutes les équipes ont également été conviés à élaborer leurs propres cartes Système de manière indépendante, occasionnant la production de 16 nouvelles cartes supplémentaires.

Une deuxième série de résultats a été associée aux façons d'améliorer la méthodologie du jeu. Il était manifeste que le processus en deux étapes utilisé dans la première partie, i) le remue-ménages et ii) l'utilisation d'équipes rouges fondée sur la confrontation a joué un rôle-clé

dans la promotion d'idées novatrices. L'utilisation d'équipes rouges fondée sur la confrontation a permis de mettre en évidence les vulnérabilités dans les cartes. Une méta-analyse approfondie de la première partie du jeu a indiqué que cela pourrait être affiné grâce à un processus en trois étapes avec l'ajout d'une séance commune où les équipes rouges et mauves renforcent mutuellement les cartes IdS. Cette modification à la méthodologie devrait donner lieu à une solide série de cartes IdS, plutôt qu'en une tentative par les équipes de « remporter » le jeu.

Signification : La première partie du jeu MAD a permis de concevoir des idées pour les systèmes Horizon II et III qui exploitent les technologies potentiellement perturbatrices. L'étendue selon laquelle ces idées influenceront sur la planification de la R & D de RDDC sera connue au moment de la réalisation de la deuxième partie. RDDC et le personnel des FC ont activement participé au processus et sont d'avis qu'il s'agissait d'une entreprise digne de ce nom. En outre, la première partie a démontré l'utilité de la méthode d'équipes rouges afin de produire de meilleures cartes IdS et de favoriser l'échange sur les idées en lien avec les technologies futuristes parmi les participants provenant de différents centres de RDDC.

Plans futurs : Les cartes IdS élaborées dans le cadre de la première partie seront évaluées en fonction de leur potentiel de perturbation dans la deuxième partie des jeux MAD qui se tiendra au début de 2011. Cette deuxième partie consistera en un exercice de jeu de guerre où les équipes rouge et bleue des FC élaboreront des plans d'action en vue d'atteindre les objectifs assignés de la mission. Ces équipes recevront des cartes IdS afin d'établir quelles sont les cartes qui perturbent les plans d'action de l'équipe. Le potentiel de perturbation d'une carte reposera sur la différence dans les plans d'action en présence et en l'absence des cartes Système. Les première et deuxième parties réunies pèseront sur les décisions d'investissements rattachées au cycle de vie des technologies potentiellement perturbatrices.

This page intentionally left blank.

Table of contents

Abstract	i
Résumé	i
Executive summary	iii
Sommaire	v
Table of contents	viii
List of figures	x
List of tables	xi
Acknowledgements	xii
1 Introduction.....	1
2 Results.....	4
2.1 IoS cards produced in response to vignettes.....	4
2.1.1 Vignette 1 – CF-led quick reaction force to secure kidnapped VIP.....	5
2.1.2 Vignette 2 – Crowd control / situational awareness operations in camps for displaced peoples.....	7
2.1.3 Vignette 3 – Attacks on CF operational C2 systems (possibly from sympathizers in home countries).....	9
2.1.4 Vignette 4 – Conduct counter-piracy operations using joint capabilities	10
2.1.5 Vignette 5 – Security for reconstruction of transportation corridor.....	12
2.2 Idea of System Cards produced by individual participants	14
3 Feedback	17
3.1 Judgments and Insights from the Players	17
3.1.1 Nature of confrontation between Purple and Red teams.....	17
3.1.2 Scenarios	17
3.1.3 Vignettes	17
3.2 Feedback Forms.....	18
3.2.1 Question 1: Did MAD Part I enable the development of systems using PDT?	19
3.2.2 Question 2: How would you run the MAD Part I differently?.....	19
3.2.3 Question 3: How would you suggest that IoS cards are developed in the future and who should develop them?.....	20
3.2.4 General comments.....	20
4 Meta - analysis.....	21
4.1 Meta-analysis of the game output.....	21
4.2 Meta-analysis of the gaming methodology	21
4.2.1 MAD Part I gaming methodology.....	21
4.2.2 Red-teaming, competition and innovation	22
5 Summary	24

References	25
Annex A ..Potentially disruptive technologies.....	27
Annex B ..Horn of Africa scenario given to participants.....	29
Annex C ..Sample IoS cards	35
Annex D ..Excerpts from the 26 feedback forms returned.....	36
List of abbreviations	39
Distribution list.....	42

List of figures

Figure 1: Schematic description of MAD Game Part 1.....	2
---	---

List of tables

Table 1: Potentially Disruptive Technologies and Abbreviations.....	4
Table 2: IoS Cards produced in response to Vignette 1	5
Table 3: IoS Cards produced in response to Vignette 2	7
Table 4: IoS Cards produced in response to Vignette 3	9
Table 5: IoS Cards produced in response to Vignette 4	11
Table 6: IoS Cards produced in response to Vignette 5	12
Table 7: Potentially disruptive technologies and frequency of their occurrence in vignettes	13
Table 8: IoS Cards designed by individual participants	14
Table 9: Potential Disruptive Technologies and frequency of their being addressed in cards produced by individual participants	15

Acknowledgements

The authors would like to acknowledge DRDC Ottawa for hosting the 2010 MAD Game Part I and to Mr. Sean Daniels for facilitating participant access to the site.

The authors are grateful to all of the participants for their tremendous efforts over the two days:

- Giselle Amow (DRDC Atlantic)
- Jacqui Crebolder (DRDC Atlantic)
- Murray Dixson (DRDC CORA)
- Alan Hill (DRDC CORA)
- Douglas Pelchat (DGMPRA)
- Wayne Ross (DGMPRA)
- Daniel Charlebois (DRDC Ottawa)
- Lauchie Scott (DRDC Ottawa)
- Barry Ford (DRDC Suffield)
- Bill Kournikakis (DRDC Suffield)
- Peter Tikuisis (DRDC Toronto)
- Michel Ducharme (DRDC Valcartier)
- Paul Harris (DRDC Valcartier)
- Maj. Daan Beijer (D Space D)
- LCdr. Mike Bourassa (DRDC Ottawa)
- Maj. Chris Comeau (CFB Kingston)
- Maj. Jim Gash (DLCD)
- Maj. Jack Hudson (CFAWC)
- Maj. John Sheahan (DLCD)
- Maj. Gurminder Singh (D Space D)

Referees

- LCol. Stephen Kostner (DDir DFSA CFD)
- LCol. Dan Drew (DRDC Suffield)
- Maj. Bob Miller (CDI)
- Eric Fournier (DDG, DRDC CORA)

1 Introduction

The mandate of ADM(S&T) of DND is to ensure the technological readiness of the Canadian Forces (CF). This includes minimizing technological surprise. In the ADM(S&T) yearly Functional Planning Guidance, ADM(S&T) identifies a list of ‘potentially disruptive technologies’ (PDT; [1]), and in the Convening Letter [2], ADM(S&T) tasks the Chief of Staff (S&T) and Chief Scientist of DRDC to develop a mechanism to assess the impact or disruption from each technology. This is not a straightforward task. Assessing the potential disruptions to operations from new technology (or novel uses of old technology) requires creative, futuristic thinking combined with a structure that supports objectivity and rigor [3, 4 and 5]. One approach to doing such an assessment is to bring together scientists and CF members in a structured brainstorming exercise and seminar wargame. The ‘Methodology for Assessing Disruptions’ (MAD) games are an example of this approach. Each MAD game consists of two parts. The 2010 MAD Part I took place in October, 2010, at DRDC Ottawa, and Part II will be held in the winter of 2011 at CF Maritime Warfare Centre (CFMWC).

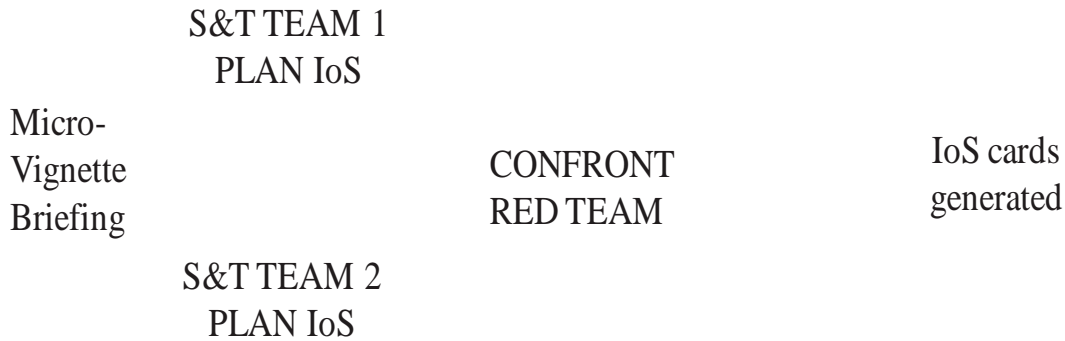
The objective of the MAD games is to assess technologies for their disruptive potential in a defence and security context through dialogue between the innovators (scientists and engineers or ‘technologists’) and the end-users (soldiers). During a MAD game, participants explore the utility of technological systems to *Blue Forces* (the CF and coalition forces, and supporting infrastructure or personnel) and countermeasures that could be adopted by a *Red Force* (adversary) to undermine their efforts. Determining the disruptive potential of technologies is often difficult because of the novelty of the way in which a technology or a system of technologies is used causes the disruption. The MAD methodology attempts to address this difficulty by developing technology ideas for real military problems in the form of an Idea of Systems card (Part I) and then providing the system concepts to a different user group to see how they might actually use them (Part II). While this process is in no way exhaustive or exclusive it provides an important tool for the investigation of PDT to complement the other more traditional studies underway within DRDC.

The consumers of the results of the MAD games are the force development community (Chief Force Development (CFD), and Chief Defence Intelligence (CDI) and DRDC. The results influence departmental investment decisions in future technologies and are used by DRDC to inform the evolution of their S&T programs as well as for disseminating and promoting (*socializing*) ideas around new technologies.

The MAD games are a *Canadianized* version of the Disruptive Technology Assessment Game (DTAG) designed by NATO [6]. The Office of the Chief Scientist, DRDC has previously run developmental versions of DTAGs in the National Capital Region [7] and at DRDC Suffield, culminating in the present structure of the MAD games.

Part I of a MAD game is a two-step process consisting of i) brainstorming and ii) red-teaming via confrontation. In Part I, scientists generate Idea of Systems (IoS) cards. These IoS cards will be used in Part II by the CF in a wargame setting. IoS cards are usually single page descriptions of a futuristic fielded piece of kit or ‘*softer*’ (social, diplomatic, cultural etc.) influence system. Part I is structured so that two ‘Purple’ teams composed of DRDC scientists and a military advisor compete against one another to produce the most potentially disruptive IoS cards. Purple teams

provide integrated support to the *Blue Force* in all three environments: Land, Air and Maritime independently responding to a problem(s) presented in a vignette by developing Blue force enablers in the form of IoS cards. The IoS cards thus generated are used against a Red Force composed of CF members posing as adversaries' set on thwarting Blue's plans at every turn. The Red Force is also provided with pre-set mission objectives. A schematic of the process for Part I is shown in Figure 1 (drawing courtesy Dr. Gitanjali Adlakha-Hutcheon).



Structured data capture

Figure 1: Schematic description of MAD Game Part I

An important aspect is for the teams to anticipate countermoves and try to plan three moves ahead of the adversary. Each purple team is advised by a CF officer to provide operational context. Once completed, the IoS cards are evaluated through a mock confrontation between the Purple team and the Red team. The confrontation step provides a conceptual reality check of futuristic IoS cards for their relevance to operations and also identifies vulnerabilities within systems. A team of referees presides over Part I of the game to allow/disallow moves and countermoves.

Part II of the MAD games is structured to resemble a conventional seminar wargame where Red and Blue teams composed of CF officers and scientific advisor's develop Courses of Action (COA) and then are provided with IoS cards to determine which cards disrupt a team's COA. Names of interested participants from the Purple teams will be drawn for participation in Part II as scientific advisors to the Blue and the Red teams. Part II will also have an observation team composed of the Team MAD (organizers of MAD games) and selected participants of Part I to provide continuity between the two parts of the MAD game.

The MAD Part I game at DRDC Ottawa focused on a subset of 7 (Annex A) of the 11 potentially disruptive technologies listed in the 2010 Functional Planning Guidance (FPG; [1]). These technologies include: Quantum Capabilities; Micro-Satellites; Virtual Reality and Neural-interfaces; Non-conventional Weapons; Novel Power Sources; Biology-based Solutions (Biometrics, Bio-signatures, and Broad-spectrum Therapies); and Internet-based Social Networking. The MAD games along with expert analyses are an integral part of the assessment phase of the PDT Life cycle process established by the Office of the Chief Scientist in response to the ADM (S&T) Functional Planning Guidance [1] and Convening Letter [2]. These 2010 PDT areas have also each been assigned to a DRDC centre for analyses by experts.

This Technical Memorandum describes Part I of the MAD games held at DRDC Ottawa on October 5 & 6, 2010. Within the document Section 2 reports the results; and feedback from participants is presented in Section 3. Feedback was solicited in two forms: first through a verbal session referred to as Judgments and Insights and second through feedback forms. The analysis of these results is presented in Section 4 where recommendations are made for improving Part I of future MAD games. The conclusions are provided in Section 5.

2 Results

The primary output expected from 2010 MAD Part I was the creation of IoS cards. MAD Part I was designed to solicit IoS cards through two processes: 1) a structured brainstorming within teams triggered in response to various vignettes followed by 2) a session in which participants were invited to develop their personal ideas outside of their assigned teams. The two Purple teams (formed of S&T professionals and a military operational advisor) together developed a total of 18 IoS cards. The Red team (comprised of military operators and a scientific advisor) developed 13 IoS cards and the individual IoS card portion of Part I yielded 16 new cards. These results will be elaborated below in two sub-sections. The IoS cards generated in response to the vignettes are described in sub-section 2.1 and the session for the creation of cards by individual participants is discussed in sub-section 2.2.

2.1 IoS cards produced in response to vignettes

The primary objective for the Purple teams was to produce IoS cards within seven PDT areas (Annex A) in support of Blue Force operations. The IoS cards were to be designed in time Horizon II and III that is to say 10 years in to the future from 2020, the time of play (2020-2030). The role of the Red Force was to counter the IoS cards by ‘punching holes’ in them. The ‘Horn of Africa’ scenario highlights an asymmetric conflict in the Somaliland and Puntland regions of Somalia in the year 2020 [8]. Five tactical vignettes were played within the context of this scenario. Salient features of the scenario were provided to all participants as part of their read-ahead package (Annex A and B). For each vignette the Purple and Red teams were provided the effects desired off of the Blue and Red forces respectively.

The IoS cards produced in response to each vignette played are discussed from the perspective of the moves by the Purple teams and countermoves by the Red team. Two sample IoS cards are also shown in Annex C. Also reported for the IoS cards are the PDT areas that they lend themselves to for each of the five vignettes played.

Tabulated below are the PDTs and the abbreviations assigned to them (Table 1).

Table 1: Potentially Disruptive Technologies and Abbreviations

Potentially Disruptive Technologies	Abbreviations
Quantum Capabilities	QuC
Micro-satellites	MiS
Virtual Reality and Neuro-interfaces	VRN
Non-conventional Weapons	NCW
Novel Power Source	NPS
Biology-based Solutions	BbS
Internet-based Social Networking	ISN
Other New Technologies not among the PDT	ONT

The following sub-sections describe the IoS cards that were generated in response to each of the five vignettes played along with the way in which the IoS cards were used and countered.

2.1.1 Vignette 1 – CF-led quick reaction force to secure kidnapped VIP

Setting: “An immediate challenge facing the Somaliland defence force is the ongoing low intensity border dispute with Puntland and the various insurgent groups acting against the government in Hargeisa. This conflict has at times overwhelmed African Union (AU) peacekeeping forces on both sides of the Somaliland-Puntland border, as well as Somaliland defence force units. This has been the prime driver for the requirement of a CF-led quick reaction force, which can respond to deteriorating tactical situations to support AU forces with Intelligence Surveillance Target Acquisition Reconnaissance (ISTAR) and combat capabilities, and facilitate withdrawal of casualties while remaining cognizant of the necessity for a relatively low footprint. Although Puntland has not rescinded its claim on the disputed area, for the past number of years it has respected the peace and has not taken any overt military action across the demarcated border.”

“Provide a Quick Reaction Force (QRF) of sufficient capability to support Somaliland and AU forces, and, if necessary, to conduct combat operations autonomously on an occasional basis, and provide military security as required for Government of Canada (GoC) mission elements ... As required, lead or provide support in the disbandment of any illegal armed group ... conduct autonomous anti- and counter-terrorist operations in coordination with allied theatre command”

A report has been received from AU forces in Sanaag that they are facing a significant (100+) force that has captured a regional VIP. The force which has no overt linkage with Puntland or Somalia government is advancing on the AU forces in a convoy intending to take the VIP across the border into Puntland. AU forces are insufficient to oppose this event. Total size and capability of opposing force is uncertain, morale of AU force is low. Should the Red force succeed, support from local regional groups will be negatively impacted. Intelligence indicates that the opposing force is well informed of the AU capabilities and their likely call for QRF support.

In this vignette, the desired effects solicited from the Blue force were to 1) secure the kidnapped VIP and block the convoy of Red insurgents from gaining entry into Puntland; 2) provide surveillance of the disputed border region; and 3) to provide Command and Control (C2) for the VIP rescue operation.

The Red force desired effects were to 1) provoke conflict in the disputed border region; 2) disrupt local regional group support for AU Forces and the CF; and 3) pre-empt and disrupt local security forces.

The IoS cards generated during Vignette 1 are shown in Table 2.

Table 2: IoS Cards produced in response to Vignette 1

Team	IoS ID	Name of IoS Card	Basic Function	PDTs addressed
Purple 1	V1P1-1	Quantum Tech Microsatellites	Surveillance of disputed region	QuC, MiS
	V1P1-2	Non-lethal mass sedation technology	Support extraction of VIP	NCW, BbS
	V1P1-3	Deployable location-based network	Track VIP	BbS
Purple 2	V1P2-1	Swarming Micro ARray Technology (SMART)	Support rescue of VIP from convoy	NCW, BbS
Red	V1R-1	Sleeping man switch-remote	Thwarts attempted rescue by killing VIP	NCW
	V1R-2	Attack on fuel	Contaminate or deny use of combustion engines	Pre-existing
	V1R-3	Attack on water supply	Create chaos to deter and demoralize blue	Pre-existing

Summary of play of vignette 1: The Purple 1 team concentrated on detecting the whereabouts of the VIP (V1P1-1) and non-lethal neutralization of the Red force (V1P1-2) to enable retrieval of the VIP by CF forces, under a net of surveillance to provide situational awareness (SA) on Red movements (V1P1-3). General area surveillance relied on microsatellites and quantum sensing to achieve less than one meter resolution. Detection involved a biochip that was pre-implanted in the VIP which was detectable by a deployed array of ground-based sensors.

The Purple 2 team took a similar approach to the challenge. They also employed a tagging technology to mark the VIP, albeit utilized radio frequency identification (RFID) instead of a biochip implant, and employed an array of sensors to gather situational awareness on Red to find, via detection of the tag, the location of the VIP. The main difference was that the sensor array itself had swarming capabilities and was capable of delivering a non-lethal attack to neutralize Red and enable the recovery of the VIP (V1P2-1). In essence, the card produced by Purple 2 was largely an integrated version of the three separate IoS cards created by Purple 1, apart from some differences in the chosen capability delivery mechanism (technology).

The Red team countered the non-lethal weapons (NLWs) employed by the Purple teams through use of a device that will kill the VIP when in the presence of the non-lethal, electromagnetic pulses (EMP; V1R-1). Thus if Purple tried to knock out Red, and consequently the VIP, the VIP would be killed. Red also schemed to confound the recovery operation by attacking Blue's fuel supply (V1R-2) and preventing AU involvement through demoralization and creation of general chaos (V1R-3).

During the back-and-forth portion of the Red and Purple confrontations, several rebuttals to the IoS cards surfaced. Red stated that they could call upon a technologically advanced nation that is sympathetic to their cause to deny service to Blue satellites (V1P1-1). Purple Team 1 questioned Red's assumption to be able to call upon such services from said nation.

Red also noted that mass sedation of a moving convoy could be dangerous to the VIP (counter to VIP1-2 and VIP2-1). Purple acknowledged that the Blue Force can select the timing of the attack to minimize adverse effects, but in the end they would have to accept the possibility of collateral damage.

Red noted that they could shield electromagnetic signals emanating from the VIP's. Red also intended to spread out their convoy to make it more difficult for Blue to both detect the VIP and to use their non-lethal weapons. Red also noted that they could destroy the ground based surveillance network beforehand or motivate the population to destroy it. Purple 1 noted that Blue could conceivably cloak or otherwise disguise the ground-based surveillance network. Also, Purple mentioned that Blue could harden the airborne surveillance nodes from an electromagnetic pulse-style attack, but Red questioned whether it could be done cheaply and in such a way that the sensor would remain light enough for flight. Finally, Purple 1 noted that Red may jam the ground-based network, but that Blue would have other more conventional methods of gathering situational awareness (e.g. optical means for line of sight detection).

2.1.2 Vignette 2 – Crowd control / situational awareness operations in camps for displaced peoples

Setting: “Refugees from throughout the Horn region seeking support from non-governmental organizations (NGO) operating in Somaliland have formed tent cities around some of the urban centres and the people there lack many basic necessities. Although NGO's have been managing to care for the refugees, any change to the status quo may very well lead to a situation requiring CF assistance.”

Recent cuts in funding, by western governments, to key NGO operating in the refugee camps about the capital have resulted in a reduction in services and increased unrest. Over the past two days the medical community have seen an increase in the number of people reporting flu-like symptoms in the camps, and patrols report increased numbers of funerals. On the web, a number of fringe groups are calling the decreased funding and increased sickness a plot by the government to solve the displaced person problem.

The Blue Force desired effects were to 1) maintain local regional group support for the government, AU Forces, and the CF; 2) maintain situational awareness with robust command and control (C2) at the refugee camp; and 3) detect and disrupt or prevent any insurgency-backed uprisings.

The Red Force objectives were to 1) generate support for the insurgency from local regional groups; 2) misinform refugees and local nationals in order to undermine Blue; and 3) instigate unrest and violence at the refugee camp.

The IoS cards generated during Vignette 2 are shown in Table 3.

Table 3: IoS Cards produced in response to Vignette 2

Team	IoS ID	Name of IoS Card	Basic Function	PDTs addressed

Purple 1	V2P1-1	High mobility water / drug / food delivery mechanism	Buffer against human necessity shortages and epidemics, reduce insurgency support	ONT
	V2P1-2	Advanced Social Network Monitoring	Situational awareness of extremist/insurgent activity	ISN
Purple 2	V2P2-1	Real-time social network analysis	Situational awareness of crowd intent	ISN
	V2P2-2	Biometric analysis	Situational awareness of crowd intent	BbS, possibly MS or ONT
Red	V2R-1	Evil PA Game/atrocities: Free Inoculation of local leaders	Gifts to generate local support for insurgency	BbS, pre-existing
	V2R-2	Especially evil PA Game/atrocities: Propaganda campaign	Misinform refugees that Blue is committing atrocities	ISN, pre-existing

Summary of play of vignette 2: The Purple 1 team initially concentrated on attacking what they considered the source of the problems in the refugee camp, namely, lack of food, clean water, insufficient sanitation, and medical facilities. The resulting IoS card (V2P1-1) laid out a high-mobility water, food and drug delivery mechanism with capabilities to aid sanitation as well. The idea was to use a lightweight, flexible piping material to deliver clean water (via filtration), nutrients dissolved in the water to bolster refugee's state of health, and dissolved medicines where and when applicable. The same type of piping could be used to carry away wastes, and would be self-healing and monitored to detect tampering with the pipes. The entire piping/filtration/sanitation package was envisioned to fit on a single C-17¹. A second IoS card (V2P1-2) outlined a system for advanced social network monitoring and analysis to keep pace with and forewarn of possible extremist threats in the region, both real and perceived.

The Purple 2 team concentrated their efforts on real-time social network monitoring (V2P2-1) and biometric analysis (V2P2-2). The former IoS card would collect and collate the communication patterns within/without the camp area and provide content/context analysis and anomaly detection. The second card, biometric analysis, would detect the physical location and movement of masses, have a pre-established (normal) reaction baseline to compare such patterns tracked through bio signature detection (e.g. thermal) using space or airborne sensors (optical and infrared), backed by automatic analysis of data and anomaly detection. Advanced cueing of events would allow for proactive response and the identification of provocateurs.

The Red team questioned whether or not displaced people in the population would trust Blue aid given that they (Red) were scheming to bolster support for insurgency by building relationships with local leaders receiving direct profit from Red (e.g., vaccines, viagra), and/or by staging and broadcasting atrocities committed by the AU achieved through similar means (bribes, etc.).

¹ Other related concepts discussed (although not on the final version of the card) included advanced drilling equipment to create wells where needed, thus adding redundancy to the water distribution, and high production 'portable gardens' or other such means to generate high protein food locally to further decrease reliance on supply chains.

With regard to the piping technology card (V2P1-1), Red also noted that in certain African localities the inhabitants are willing to go to extreme lengths to avoid drinking water that tasted different from the water that they were used to drinking. Red’s rebuttal to technology that determines crowd intent (cards V2P1-2, V2P2-1, V2P2-2), either through social network flow or biometrics, was that Blue needs a baseline on crowd intent technologies, which is difficult to obtain. Red could, in principle, keep creating disturbances to confound Blue forces ability to establish a baseline.

2.1.3 Vignette 3 – Attacks on CF operational C2 systems (possibly from sympathizers in home countries)

Setting: “People who are often highly educated, technologically savvy, and physically located within Canada and allied countries, also conduct supporting cyber attacks on national, UN, and NATO networks, including attempts to disrupt and interdict military operational and tactical level C2 systems. These attacks include attempts to interdict systems required for the operation of network-reliant platforms such as semi-autonomous and traditional unmanned aerial vehicles (UAV), manned aircraft, naval vessels, and land combat systems. While poorly coordinated with tactical-level activities of extremists in the Horn, these attacks have the potential for severely hampering allied operations. On the other hand, the creation and dissemination of propaganda by these supporters has created an almost minute-to-minute ‘news cycle’ that manages to influence global and local African target audiences as well as the domestic publics of the UN and NATO contributing states.”

The Blue Force objectives were to 1) monitor and defend operational and tactical level networks; 2) maintain positive C2 & ISTAR capabilities; 3) develop a contingency plan to mitigate disruption or loss of primary C2 nodes; and 4) deny Red Force situational awareness.

The desired effects for the Red Force were to 1) destroy Blue Force cohesion by attacking their critical C2 nodes; 2) maintain situational awareness (SA) via social networking and streaming; and 3) maintain local regional groups’ support to insurgency.

The IoS cards generated during Vignette 3 are shown in Table 4.

Table 4: IoS Cards produced in response to Vignette 3

Team	IoS ID	Name of IoS Card	Basic Function	PDTs addressed
Purple 1	V3P1-1	Domestic Electronic Adversary Threat (DEATH)	Finds domestic supporters and attacks their computers	QuC, ONT
Purple 2	V3P2-1	Integrated network infrastructure	Provides almost total cyber-defence of operational C2	BbS, ONT
Red	V3R-1	More evil: kinetic attack on cyber-based services	Destroy (disrupt) Blue Force cohesion by attacking their critical C2 nodes	NCW, Pre-existing
	V3R-2	Not really evil: non-cyber social networking	Maintain local regional groups’ support to insurgency	ISN, Pre-existing, ONT

	V3R-3	Less evil: virus attacks inserted at point of production	Create vulnerabilities in Blue technology	Pre-existing
--	-------	--	---	--------------

Summary of play of vignette 3: The Purple 1 team opened play with an IoS card that featured a self-protecting network with an artificial intelligence (AI) immune system against computer viruses that, overall, functioned analogously to a human immune system against pathogens (V3P1-1). This immune system had an additional, aggressive feature that would seek out machines that were attempting to hack into the system and neutralize them (deactivate power supply fans, overclock PCs, etc.). Quantum encryption and quantum computing would also be employed to protect networks and to perform enormous computations extremely quickly. Furthermore, optical computer systems would be used to act as a technological “transition” through which traditional technologies had to pass in order to connect to other systems, creating an additional kind of technological barrier for Red to overcome.

The Purple 2 team presented an IoS card that it claimed would provide almost total cyber defence of operational C2 networks (card V3P2-1). The technologies employed involved encryption (non-quantum), policy-based access management, biometrics for authentication and access control (facial, presence, etc), trusted labeling and trusted auditing, digital signatures, network sensors for intrusion detection and prevention, virus scans, and firewalls. In addition, the network would provide redundant services and use robust and rugged hardware (trusted hardware).

The Red team acknowledged that operational C2 can be protected, but questioned whether the larger internet would be so protected. Red also noted that the systems were vulnerable to EMP attacks. Purple 2 teams’ rebuttal was that at least undersea optical fibers would be safe from EMP.

Red’s counter to the aggressive portion of Purple’s ‘DEATH’ IoS card (V3P1-1) was to make the attack look like it was coming from another machine. This can result in a Blue ‘self-attack’ if Red is using zombie machines. Purple responded that if Red is already past the line of defence, then that is a possibility that has to be examined. Purple also acknowledged the possibility of collateral damage to machines used for cyber attacks without the owner’s knowledge.

2.1.4 Vignette 4 – Conduct counter-piracy operations using joint capabilities

Setting: “A primary concern in the maritime domain is the strategic choke point of the Bab-el-Mandeb and the traffic flow through the Gulf of Aden. Although there are few incidents of piracy in Somaliland territorial waters, it is still a problem in the larger region. Ships have been attacked in the Gulf of Aden, the Indian Ocean and around the Seychelles. Whereas the CF mission in Somaliland is centered on Somaliland sovereignty, support to the wider and ongoing counter-piracy campaign is imperative. The fact that counter-piracy operations in the Horn area exist highlights the need for more than a policing solution at sea. The overall stabilization of the area will remove safe havens for pirate organizations to operate from. Somaliland is used by many nations operating as part of the NATO/ United Nations Mission Horn of Africa (NUNHOA) mission to transfer captured pirates for prosecution.”

The Blue Force objectives are to 1) deny safe-havens for piracy operations; 2) embolden Somaliland economy and sovereignty; and 3) foster cooperation across environments (Land, Air, Sea) / forces (AU, CF).

The Red Force objectives are to 1) create regional economic instability; and 2) gain funding through selling cargo and VIP ransoms.

The IoS cards generated during Vignette 4 are shown in Table 5.

Table 5: IoS Cards produced in response to Vignette 4

Team	IoS ID	Name of IoS Card	Basic Function	PDTs addressed
Purple 1	V4P1-1	Jolly Roger's Angry Parrots	Protect ships by swarm-attacking non-tagged invaders (friendlies are all tagged)	BbS, ONT
	V4P1-2	Jolly Roger's Talking Parrots	Track tagged individuals identified as potential pirates back to port and share information with local forces	BbS
Purple 2	V4P2-1	Nano-modified fuel	Turns to gel when triggered with remote signal (stops pirate ships)	ONT
	V4P2-2	Persistent surveillance (Golden eye)	Diminish safe havens	Pre-existing, ONT
	V4P2-3	Swarmboats	Provide protection to commercial vessels	ONT
Red	V4R-1	Semi-devious: be nasty pirates (stealth technology)	Smuggle captured VIPs, ransom everything	ONT
	V4R-2	Devious: Disrupt navigation with UAVs	UAVs carry EMP or CBR threat	NCW, ONT
	V4R-3	Really devious: Disrupt navigation with sea-based IEDs	Destroy vessels	ONT (variation of pre-existing)

Summary of play of vignette 4: The Purple 1 team suggested using a swarm of 'bots' or micro-UAVs, combined with RFID tagging technology, to both biometrically (or otherwise) identify crew members and protect against unwanted intruders (V4P1-1). The micro-UAVs would be capable of delivering lethal or non-lethal neutralizing effects on persons boarding the vessel. In addition, suspicious and/or unknown individuals or vessels could be tagged (V4P1-2) and traced back to safe havens. This information would be passed on to local authorities, enabling them to deal with the threat. Both technologies would be available for use via commercial manufacturing and distribution.

The Purple 2 team proposed to ensure that only nano-modified fuel was available to local inhabitants of the area. The fuel could be triggered to harden into a gel by CF and Allied forces,

thus disabling any suspicious, approaching vessels (V4P2-1). A second line of defence against boarding consisted of ‘swarmboats’ capable of attacking and neutralizing approaching vessels at sufficient standoff (V4P2-3). Lastly, dirigibles and towers would provide persistent surveillance to enable detection of piracy and tracking the vessels involved to port (V4P2-2).

Red countered that they would engage in high technology-based smuggling and VIP ransom type operations, employing stealth technologies and patterns of movement/behavior. This would make Red difficult to distinguish from common fishermen, even going so far as to bribe fisherman to change their own patterns. The criminal organization could even evolve to one that provides ‘protection’ from disruption for a fee (e.g., Mafia style). Red also contended that they would hack into navigation and control systems to disrupt vessel traffic in the area (V4R1-1). Red also suggested disrupting sea traffic via UAV-based EMP and chemical, biological, radiological (CBR) threats, in addition to sea-based improvised explosive device (IED)-style threats. Further havoc would be wreaked by causing oil spills and bio-contamination of cargo (including medicine; V4R-2, V4R-3).

The Red team’s rebuttal to nano-modified fuel was that this technology also could be used by Red to stop intended target vessels if the nano-bots were in Blue fuel and Red discovered the trigger. On the other hand, Purple noted that they (Blue) would have the antidote on hand.

2.1.5 Vignette 5 – Security for reconstruction of transportation corridor

Setting: “Two key elements to the Government of Canada (GoC) plan involve provision of support to the AU peacekeeping mission between the border of Puntland and Somaliland and the reconstruction and expansion of the Addis Ababa - Berbera transportation corridor.”

“Provide engineering support to enhance efforts to develop the Addis Ababa-Berbera transportation corridor when and as requested by other GoC, Somaliland, United Nations (UN), and AU agencies”.

The objectives of the Blue Force were to 1) strengthen security forces cooperation and interoperability; 2) renew infrastructure for modern commerce and trade; and 3) embolden the Somaliland economy and sovereignty.

The objectives of the Red force were to 1) create regional economic instability; and 2) disrupt security operations (contractual, AU, UN, CF).

The IoS cards generated during Vignette 5 are shown in Table 6.

Table 6: IoS Cards produced in response to Vignette 5

Team	IoS ID	Name of IoS Card	Basic Function	PDTs addressed
Purple 1	V5P1-1	Roboroad	Sense traffic density/location, threats via towers, provide comm., easily repaired	ONT
Purple 2	V5P2-1	Corridor as sensor (Smart corridor)	Sensing all aspects of traffic along the roads.	QuC

	V5P2-2	Drive-through scanners	Detect threats in vehicles	VRN, ONT
Red	V5R-1	Banks are bad	Attack banking system to destabilize the area	ISN, Pre-existing
	V5R-2	Bowling for purple	Physical attack of roads using nano dust, etc.	ONT

Summary of play of vignette 5: The Purple 1 team devised a card about a roadway that is easy to construct, repair (possibly self-repairing), has built-in and adjacent sensing capabilities, and deploys humans and automated robotics for standing and roving patrols, and also to query stopped vehicles (V5P1-1). The road itself would be composed of a spray on (self-leveling) material, one idea being a polymer that turns local sand into a firm roadway. The designers would encourage cell-phone communication to identify any threats perceived by drivers, and there would be a rapid response force to deal with such threats. Sensors built into the road would relay traffic information and cell-phone towers along the corridor would both relay signals and carry sensors to detect threats (e.g., CBRN).

The Purple 2 team also envisioned a ‘smart’ road characterized as a layered ‘electronic sensor tunnel’ (V5P2-1). The roadway enabled tamper detection anywhere in vicinity of the road with the ability to track any changes to the condition of the road (e.g., authorized vs. environmental vs. unauthorized and requiring investigation out to 100m to either side of the road. Acoustic sensors would be positioned along the road to detect entry at non-authorized areas or within reasonable weapon range. The road itself would be constructed of sensing materials (or painted with a sensor coating). Vehicle counters, trackers and point-of-entry control would also be provided (V5P2-2). Various scanning technologies would be employed to detect threats in vehicles travelling up to 50 km/hr as they passed through/by scanners at the points-of-entry at 100m. The VR interface would enable advanced visualization and representation of scanning imagery to aid in the detection process.

The Red team proposed to create regional economic instability by attacking the local banking system both physically and through cyberspace. This would disrupt the ability of Blue to engage contractors needed to build and maintain the roadway (V5R-1). In addition, Red schemed to disperse several varieties of nano-dust on the road (V5R-2). For instance, one type would simply dissolve away the road material. Another would accumulate on vehicles and later explode. Deployable, self-healing, smart minefields were also put forward by the Red team.

The Purple teams seemed taken aback by Red’s attack on the banking system, as they had anticipated road attacks only.

Tabulated below in Table 7 is the number of times that the seven PDT were addressed in formulating IoS cards over the course of the five vignettes. Not all of the PDT areas were drawn upon in each vignette. This was to be expected given the wide scope of the PDT areas.

Table 7: Potentially disruptive technologies and frequency of their occurrence in vignettes

Potentially Disruptive Technologies and their abbreviations	Number of vignettes in which
---	------------------------------

	PDT were addressed (out of 5)
Quantum Capabilities (QuC)	3
Micro-satellites (MiS)	2
Virtual Reality and Neuro-interfaces (VRN)	1
Non-conventional Weapons (NCW)	3
Novel Power Source (NPS)	0(3)
Biology-based Solutions (BbS)	4
Internet-based Social Networking (ISN)	3
Other New technologies (ONT)	4

2.2 Idea of System Cards produced by individual participants

After the five vignettes were played, all team participants were given the opportunity to independently create IoS cards that they had thought of outside of the teams to which they were assigned. The design of the Part I did not allow these cards to be ‘tested’ via a confrontation against the Red team.

Summarized in Table 8 are sixteen IoS cards produced during the post-vignette session on IoS card creation by participants. In addition the basic function served by the card and the PDT it addressed are also tabulated.

Table 8: IoS Cards designed by individual participants

IoS ID	Name of the IoS Card	Basic Function	PDT addressed
I1	Auto-display of tactical picture	Auto enlargement of portions of tactical display in response to alerts.	ONT
I2	Micro-polymer entrapment film	Surface-active coating which is reactive to contact released by signal. Prevent tampering of gear supplies	ONT
I3	Individual water purification	Man portable reliable water purification.	NPS, BbS, ONT
I4	Alternate Food Source	Replace requirement for consuming IMP meal, cutting down on weight carried and resupply frequency.	BbS
I5	Real-time Influence Operations	Real-time monitoring of all global electronic media with capability to disrupt and/or interrupt transmission with counter-messaging	ISN
I6	Paint-on Cameras	Paintable optical or infra-red sensors that can be applied to many objects and the signals combined to provide high fidelity pictures.	ONT

I7	Network of things	Surface treatment that provides a network node with integrated power generation	ONT NPS
I8	Deployable renewable power generation	Self-contained green power generation system	NPS
I9	Location based Network Bomb	Explosive that is activated by a unique RF signature	ONT, NPS
I10	Non-RFID biometric	Recognition by character	BbS
I11	Inoculation Tunnel	Aerosol borne inoculation – portable walk-through tunnel	BbS
I12	Idiot's IDE	Cellphone based trigger that can replace standard NATO munitions' trigger on standard munitions like hand-grenades	Pre-existing
I13	Omnipotent communicator	Very light weight, low power, low cost, interoperable, multi-level security	ONT, NPS
I14	Dark Energy Exploitation	Unlimited power supply based upon dark energy	NPS, ONT
I15	Bacteria based fuel source	Freeze-dried bacteria that produces fuel when added to reactant like water	NPS, BbS
I16	Assisted targeting for Infantry	Optimizes firing of weapon after trigger pulled to make all soldiers equivalent of a sniper. Essentially compensates for lack of training by taking over the weapon fire timing.	VRN, ONT

Tabulated in Table 9 is the frequency of occurrence of PDT in cards produced by individual participants. The PDT addressed most frequently was novel power sources (NPS). Under the “other” category the use of nano materials as a component of surface materials was also popular. The popularity of novel power supplies is interesting in that while it was not the primary technology used during the development of cards within the vignette play it was acknowledged to be a critical underlying technology for many of them. This observation may signal an anecdotal disruption from the perspective of technological systems required to enable functionality of futurist systems.

Table 9: Potential Disruptive Technologies and frequency of their being addressed in cards produced by individual participants

Potentially Disruptive Technology Areas	Number of independent IoS cards in which PDT was addressed (out of 16)
Quantum Capabilities (QuC)	0
Micro-satellites (MiS)	0
Virtual Reality and Neuro-interfaces (VRN)	1

Non-conventional Weapons (NCW)	0
Novel Power Source (NPS)	7
Biology-based Solutions (BbS)	5
Internet-based Social Networking (ISN)	1
Other New Technologies (ONT)	8

3 Feedback

Feedback was solicited from participants in two formats, via a verbal session referred to as “Judgments and Insights” and formally through feedback forms.

3.1 Judgments and Insights from the Players

At the end of the ‘play’ (of five vignettes and the design of IoS cards by individual participants) a Judgments and Insights (J&I) session was held. During a J&I session participants are invited to share their opinions on the game play in a free-form verbal format. J&I sessions are common within the synthetic environment (SE) community, for instance the following DRDC TMs note the use of J&I sessions to record aspects of game play, synthetic equipment performance, or other factors deemed especially relevant to success or failure from the players perspective [9,10]. Often such aspects are not or cannot be recorded automatically by the SE data stream, for example, the reasoning behind certain decisions made during game play. Therefore this format also provides immediate feedback to the participants. This session was new to majority of the MAD Part I participants and was included to capture feedback that may have been missed in the written feedback form format. J&I focused on participant perspective and could in the future be used to obtain feedback from the organizers. The main points raised at the J&I are elaborated in the sub-sections below.

3.1.1 Nature of confrontation between Purple and Red teams

It was felt that Purple and Red did not often meet ‘head to head’ in the confrontations, but rather side-stepped one another. Some believed that the game should be designed to ensure directed confrontations to put the proposed technologies through vigorous testing, whereas others believed it would be too confining and pointed out that such a phenomenon is not uncommon in warfare.

3.1.2 Scenarios

Another comment was that the overall scenario was expeditionary in nature. A suggestion was made to include an Arctic scenario in future iterations of MAD Part I.

One participant voiced the opinion that the scenario used for play did not adequately lend itself to the ‘softer’ i.e. cultural, societal or psychological, solutions for conflicts. It was their belief that such types of moderations of conflict were becoming increasingly important in the context of operations.

3.1.3 Vignettes

Elaborated below are observations associated with each of the vignettes:

Securing the release of the kidnapped VIP vignette (#1) led to the comment that the Red team should have had severely limited access to technology relative to the Blue team. This observation

is interesting for two reasons. First, even today one notes that around the world insurgencies have access to procuring top of the line commercial technologies and secondly the teams were asked to situate themselves in 2020. In regard to the latter point one might argue that by 2020 globalization of S&T would render even faster access to technology than currently.

The Crowd Control vignette (#2) prompted comments on the fact that innovation often comes from a merger of two technologies, and that this fact needs to be considered in the game. Reviewing the IoS cards, however, reveals several instances of combining technologies to create a new functionality, indicating at least a partial capture of such hybrids. The convergence of biometric and sensing technologies is one such example.

The Cyber Attack vignette (#3) inspired three comments. The first was that the vignette was difficult to act upon for those not involved in computer security. The second observer believed that the vignette was not futuristic, but rather highlighted a more conventional problem of today. The third speaker noted that the CF already has a ‘solution in the pipe’ and is not currently thinking of ‘anything else’.

The Counter-piracy vignette (#4) brought on complaints that Red seemed to have access to more resources and technology than would be expected. Since there were no strict limits placed on the resources, Red played within limits established for this game. Also, the legality of using the technologies suggested by Purple, especially in international waters, was questioned.

The Security for Reconstruction of a Transportation Corridor vignette (#5) brought on comments as well. Purple observed that they clearly prevented Red from attacking the road. It was also noted that this type of vignette has implications for countering similar threats in Canada. Red’s attack on the banking system instead of the roadway was questioned, however a Red team member rebutted that the tactic was an alternative way of achieving the goal of creating instability in the region.

3.2 Feedback Forms

Feedback forms were made available from the end of the first day until the close of the game on the following day to all participants. Referees and observers too were encouraged to fill out these forms. The following three questions were posed in the feedback forms:

1. Did MAD Part I enable the development of systems using PDT?
2. How would you run the MAD Part I differently?
3. How would you suggest that IoS cards be developed in the future and who should develop them?

In addition, participants were given space to elaborate on any other aspect of the game. A total of twenty-six feedback forms were received. At least two participants filled out the form separately for the first and second days.

Point-form lists of the raw comments, sorted by question, are included in Annex D. The subsections below summarize the feedback received.

3.2.1 Question 1: Did MAD Part I enable the development of systems using PDT?

The response to this question was varied, it ranged from nine Yes, six Maybe, seven No, to four that left the question unanswered. The qualifications associated with the perhaps and negative responses were predominantly associated with wanting the time to refine the cards further. At least two of these participants brought up the suggestion of having a second round of facing the Red team as a way to help polish the cards and improve the gaming methodology. Other qualified responses expressed reservations that such systems would or could steer investment decisions unless managers had had a chance to see the game process at play.

3.2.2 Question 2: How would you run the MAD Part I differently?

The responses to this question fell roughly into the following five categories:

1. Vignette Descriptions – participants were of the opinion that the vignettes needed to be more structured, with more details on the likes of order of battle and directly opposing desired effects for the Purple and Red teams. A couple comments were voiced regarding counterinsurgency vignettes not easily allowing for technological solutions. It was also suggested that the vignette descriptions be added to the read ahead package along with the overall scenario to initiate participant thinking on solutions.
2. Teams – participants were appreciative of the teams being composed of scientists and military advisors. An improvement proposed was to also include a military engineer in the teams. Other respondents received the small team format very well and commented on it being conducive to free play. It was also suggested that each team have a representative of another Government department especially if the vignette solution lent itself to a whole of government perspective.
3. Competitiveness – there was strong support for the game process having a confrontation between the Purple and Red teams. Participants noted that the confrontation worked best when Purple/Red were addressing the same problem, therefore, tightening up the problem description and increasing the use of the referees to keep the discussion on track were suggested. Further, several participants wanted to see the confrontation period extended to several distinct phases with some, at least small, amount of time for each side to develop a thoughtful response to the previous team's comments.
4. Card Development – while some participants noted that time limited their ability to search for pictures or references, it is worth noting that others used the time allocated following the play of vignettes to complete their set of IoS cards with references and pictures from the internet.
5. Time availability – participants would have preferred additional time to develop quality IoS cards. Suggestions to overcome this limitation included playing fewer vignettes, providing more preparation material ahead of time, and providing dedicated facilitators and note-takers for each team. It was also suggested that the

first vignette be played as a trial to give each team an appreciation of time constraints.

3.2.3 Question 3: How would you suggest that IoS cards be developed in the future and who should develop them?

Creative suggestions for developing IoS cards in the future were proposed. The foremost was for each DRDC laboratory to run the game to develop futuristic systems to support the CF. Along the same vein it was suggested that IoS cards be crafted instead of 'quad charts' for existing projects and then follow-up the 'project' IoS cards through a rebuttal with a Red team. Another idea was to have subject matter experts create such cards prior to running MAD Part I.

Alternative suggestions for who else could be involved in developing IoS cards were not proposed, reiterating satisfaction with the design of the teams for MAD Part I.

3.2.4 General comments

In most cases these comments echoed or elaborated proposals made in response to the other three questions. A range of comments on how to improve the process were provided. The general theme was that Red-teaming was useful, but the competition between Purple teams was not. Also more time was required and more resources might have been useful. Participants suggested the use of team facilitators and note-takers, more access to internet access compatible computers, and that key material be provided in hardcopy as well as electronically (vignette descriptions etc.). Participants suggested that the game be run over a longer period or with teams already in-place. A specific section needs to be added to the IoS card to state its mission and the move/countermove section removed from the front of the card prior to its use in Part II. It was also suggested that the final cards should be a combination of Red and Purple development effort. There were concerns that some good ideas got left behind because there was not enough time to explore them.

4 Meta - analysis

The MAD Games Part I of 2010 brought together 24 participants from seven DRDC centres and four CF partner organizations, namely CFD, CDI, the CF Air warfare centre and the Directorate of Land Concept Development (DLCD). A team of six put together these games.

4.1 Meta-analysis of the game output

A total of 47 IoS cards were produced as an output over the course of two days.

While IoS cards will be refined prior to playing them in MAD Part II, preliminary analysis of the cards developed by the two purple teams' revealed striking similarity in thinking. One reason for this may be that each DRDC centre sent two participants that were each assigned to different Purple teams, resulting in a roughly equivalent mix of scientific knowledge across the teams. Also, many of the common technologies that the scientific professionals referred to were referenced in the read-ahead package, which directed them to the seven PDT selected as focal points for the game. It may also result from the operational inputs to the teams by their CF advisors as they worked out what 'real' problem in the vignette needed to be solved. For example in the road scenario the Purple Team 2 advisor told their team that the problem was defence of built sections not defence of crews building roads.

4.2 Meta-analysis of the gaming methodology

MAD Part I was an incremental evolution on the original MAD concept previously developed and 'piloted' at DRDC Suffield. It should also be pointed out that the MAD differs from the NATO run DTAG in having two parts, Part I was specifically designed at DRDC to increase the utility of DTAG for Canadian purposes. Four new aspects were introduced in this Part I building on feedback received at DRDC Suffield. These are:

- Participants from all DRDC centres were included;
- Referees represented CFD, CDI and DRDC;
- The process allowed for the development of IoS cards by the Red team; and
- Participants were solicited to formulate 'individual' IoS cards.

4.2.1 MAD Part I gaming methodology

MAD Part I was played in a two-step format. In step 1 two Purple teams brainstorm and develop 'solutions' or IoS cards in response to the vignette that was briefed. This is followed by a step 2, red-teaming via confrontation between each Purple team and the Red team where confrontation enabled a critique of the IoS cards generated by the Purple teams. This second step was critical for pushing the boundaries of creative thought. Both the Purple and Red team participants were stretched beyond their traditional roles – the scientists had to create, in a short timeframe, systems using technologies outside of their primary domains of expertise and the CF officers had to wear

the hat of the adversary. It should be noted that the Red team was asked to play outside the bounds of internationally accepted conventions including the Geneva Convention.

The MAD Part I of 2010 Game marked the first time that the game was conducted as a multi-centre, multi-organization and therefore multi-disciplinary endeavor. This meant that many of the participants had never met before. Consequently, there was little basis for initial team cohesion and team building took time. This is supported by feedback that the game ran better on the second day. Additionally, anecdotal evidence suggests that the introverts expressed themselves more on the second day.

The game organizers recognized that time management would be critical for team success and consequently warned the teams in advance. In the previous MAD games held at DRDC Suffield teams were able to work through this, and in general the same was true for the teams in MAD Part I.

From the perspective of the organizers, i.e. Team MAD, it was apparent that some of the participant teams had difficulty getting organized and assigning roles, and in some cases a few personalities dominated particular discussions. As mentioned earlier, it was observed that the game ran more smoothly on the second day. It appeared that the Red team had the least difficulty with time pressure to develop the IoS cards, although they had the additional responsibility of having to respond to both Purple teams' inputs during the confrontation. They relied on their officer training to respond spontaneously. Preliminary recommendations to overcome time pressures include providing more detailed read-ahead packages and reiterating the necessity of assigning roles within teams. The organizers will analyze the feedback received further to strike a good balance between the time allocated to the teams, the expected level of effort and other variables in order to optimize the output of future iterations of MAD Part I.

4.2.2 Red-teaming, competition and innovation

One of the main objectives of the MAD game was to disseminate and promote (*socialize*) the concept of red-teaming. This was a complete success by all accounts.

Another goal of the MAD game was to promote innovation through competition between the teams. Undoubtedly, innovation took place, as is evident in the generation of an output of 47 cards in two days.

The fact that competition provided additional value was also clear from the Purple team participant feedback in their desire to optimize the winning conditions against the Red team. Modifications suggested for the confrontation phase between the Purple and Red teams are as follows:

- A tighter vignette/problem description
- A two stage confrontation with short (5 min) response development periods between moves to facilitate ordered and targeted exchanges.
- Allocating time for free-form exchange of ideas at the tail end of a confrontation after first and second order actions and reactions have been exhausted.

The extent to which confrontation between the two Purple teams advanced innovation was less obvious. Some participants took this up as a challenge while for others it proved to be a distraction. One of the referees proposed the addition of an adjudication process to facilitate competition between the Purple teams.

Purple teams were directed to create one or more IoS cards that would achieve the Blue mission objective, whereas Red tended to focus on achieving their respective mission by any available means instead of specifically targeting the Purple team's IoS card (to be assessed in Part II). While this may reflect current day adversaries that do not conform to international rules of engagement, it diluted the ability of the confrontation to lead to a more robust IoS card. A recommendation for improving the methodology is to tone down the circumvention portion and focus more on a targeted attack on the IoS. Thus the circumvention of a given IoS card is still scoped (obvious workarounds need to be identified early on) and the card itself is thoroughly tested for what it was intended to accomplish.

Participants in a future Part I thus should be directed to focus on finessing the IoS cards themselves with some operational consideration (during the confrontation phase) whereas Part II is intended to assess the IoS card in a fully-developed operational context. In order to achieve this IoS card focus in a future Part I, Red should be directed to spend considerable time attempting to achieve its goals by confronting the IoS card directly. This will be done from an 'operational' point-of-view. However, care must be taken to not allow Red to concentrate on activities that do not directly involve/engage the Purple IoS card. Red should be directed that their principal role is to 'think like the enemy' and find operational vulnerabilities or weaknesses in the IoS card and its concept of operation. The confrontation is complete when Red can no longer find vulnerabilities in the IoS card and has furthermore pointed out any obvious work-arounds. At this juncture, a third step should be added in which the Red and Purple teams jointly brainstorm solutions to the weaknesses found by Red.

The red-teaming technique can be used to include broader areas of CF operations beyond simply 'attack' and 'defend' situations as were the general themes of Part I. In the future other key operational needs of the CF such as logistics, re-supply, training, transportation etc. could be the subject of the vignettes in Part I.

Finally, it should be noted that other possible uses of the methodology employed in the MAD Part I abound within DRDC. For example, the multi-disciplinary small team process could be used to generate ideas for Technology Investment Fund (TIF) projects, or to evaluate ongoing Technology Demonstration Projects (TDP). Perhaps annual red-teaming events could be held, with inputs from all over DRDC, to analyze the effectiveness of on-going or future projects.

5 Summary

In summary improvements for playing MAD Part I in the future include:

1. Allocating a minimum of 1.5 hours for brainstorming to develop IoS cards per vignette before confrontation with the Red team.
2. Balancing the details in the vignettes such as desired effects required off each team and enabling free-play to develop IoS cards.
3. Changing the gaming methodology of Part I to a three-step process (from a two-step) where the first step is to brainstorm, second step is confrontation and the final step is for the Purple and Red teams to jointly refine the IoS card.

The 2010 iteration of MAD Game Part I was successful in harnessing the creativity of the DRDC S&T professionals in conceptualizing futuristic systems that could provide an operational advantage to our CF partners. The IoS cards developed in Part I will be assessed for their potential to provide a disruptive advantage in 2010/11 MAD Part II to be played in January 2011. The overall results of the Part I and II will inform and influence the PDT life cycle process which is a multi-year S&T outlook endeavor. The cumulative results of successive MAD games will enrich not only DRDC's knowledge and understanding of PDT but that of the entire Defence enterprise.

References

- [1] ADM (S&T) Functional Planning Guidance (2010-2011)
- [2] ADM (S&T) FY 09/10-FY 11/12 S&T Program Formulation Convening letter (2010-2011)
- [3] Echevarria II, A.J. Strategic implications of emerging technologies: Colloquium Brief, US Army War College Strategic Studies Institute,
<http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB927.pdf>, April, 2009
- [4] Wilson, J.C., Holland Smith, D. Dstl S&T Horizon Scanning White Paper (compact version 3), DSTL/0507013/3.0 March 19th, 2008
- [5] National Research Council and the Committee on Forecasting Future Disruptive Technologies, Persistent Forecasting of Disruptive Technologies, The National Academies Press, ISBN-10: 0-309-11660-0, 2009
- [6] NATO SAS-062 (2010) report on Disruptive technologies Assessment Game (DTAG) February 2010
- [7] Adlakha-Hutcheon, G. and Hubbard, P. “Disruptive Technologies Assessment Game: A pilot for DRDC and an S&T Outlook tool for assessing the disruptive potential of technological systems, DRDC Corporate TM 2010-011, December, 2010
- [8] Chukla, N, Friesen, S. Gizewski, P. Morrissey, C and Harnett, D. Expeditionary Lead Scenario: A long term stabilization campaign in the Horn of Africa Region, DRDC CORA TM 2010-174 December, 2010
- [9] Dobias, P., Sprague, K., Bassindale, S., Sinclair, D., Demaine, J. Non-lethal mixed weapon study, Non-lethal Weapons in Reactive Crowd Confrontations: CAEn Wargame Nickel Abeyance III. Unclassified (Defence Purposes Only), DRDC CORA TM 2008-046, November 2008
- [10] Sprague, K., Dobias, P., Bassindale, S., Sinclair, D., King, J., Auger-Voyer, F., Weapon System Effectiveness for the Tactical Armoured Patrol Vehicle: CAEn Wargame Nickel Scorpion. Unclassified, DRDC CORA TM 2010-107, June 2010
- [11] Maps obtained from: http://www.lib.utexas.edu/maps/africa/somalia_rel02.jpg

This page intentionally left blank.

Annex A Potentially disruptive technologies

Potentially Disruptive Technologies	
TECHNOLOGY	COMMENT
QUANTUM CAPABILITIES (DRDC Valcartier)	Includes basic quantum science as well as applied technology such as cryptography and computing).
MICRO-SATELLITES (DRDC Ottawa)	Universal access to space enabled by technologies that allow for inexpensive imaging satellites capable of 1-2 m resolution (includes both low cost low and high earth orbit launches) Spacecraft of a few centimetres in size and a few hundred grams in mass are on the horizon allowing for functional “clusters or swarms” as simple sensors, networks or persistent surveillance capabilities.
VIRTUAL REALITY AND NEURO-INTERFACES (DRDC Toronto)	The use of simulation, virtual reality and neuro-interfaces in training systems could reduce costs and provide more ‘realistic’ training. Virtual reality provides possible venues for Intelligence exploitation.
NON-CONVENTIONAL WEAPONS (DRDC CORA)	Unconventional, but non-nuclear, kinetic and non-kinetic weapons systems to meet the future needs of the defence and security partners.
NOVEL POWER SOURCE (DRDC Atlantic)	Includes bio-generation, alternate fuels, fuel cells, fusion, wireless power transmission and development of ‘Super-capacitors’ and nano-engineered devices that enable increased performance owing to their high ratio of surface area to volume.
BIOLOGY-BASED SOLUTIONS (BIOMETRICS, BIO-SIGNATURES, BROAD-SPECTRUM THERAPIES) (DRDC Suffield)	Technologies that will match sensors with an ability to identify a person by unique physical or behavioural characteristics can increase ability for surveillance of large crowds/volumes of potential adversaries/insurgents. Host of possibilities including broad spectrum gene-based therapies.
INTERNET-BASED SOCIAL NETWORKING	Networking based on information content, characterized by high accessibility and scalability, which enables new decentralized, non hierarchical, self-organizing ways of harnessing collective human efforts.

Potentially Disruptive Technologies	
TECHNOLOGY	COMMENT
(DGMPRA)	

Annex B Horn of Africa scenario given to participants

The Horn of Africa² scenario was used as the basis for the two Purple teams, supporting the Blue forces or their force developers, to identify vulnerabilities across the entire range of capabilities required to conduct missions within this scenario. These missions include the deployable headquarters concept; Canadian interagency and international coordination (whole of government (WoG) and comprehensive approach); operations in maritime, aerospace, littoral, urban and rural environments; and military contributions to host nation capability development, such as security sector reform, and the combat capabilities required to suppress and destroy enemy forces.

Horn of Africa Scenario highlights include:

1. Ethiopia represents Somaliland's most important trading partner, but corruption remains widespread and the economy is fragile plus there is a dispute with Puntland over the eastern border region;
2. A number of Arab states express their own displeasure – viewing an independent, internationally recognized Somaliland as a sign of increased US influence in the Horn;
3. Violence and instability in Somalia continues, and increasingly threatens to spill over through Puntland to Somaliland's borders;
4. There are UN humanitarian activities ongoing;
5. Deployed [African Union; AU] forces are often limited to what can be considered light infantry with little organic mobility, no air support, and weak intelligence collection and analysis, command and control, and planning capabilities. Corruption in some AU forces actually contributes to instability through participation in or facilitation of various forms of illegal activity. Because of this, the AU forces are routinely bolstered with additional capabilities from UN-member states;
6. NATO remains engaged in a number of counter-piracy missions in the Horn region;
7. Confused security environment in which the interplay between identity-driven, religious, tribal and regional violence eliminates any simple solution. Wahabbist-inspired extremists have waged a campaign of terror against civilian targets and have engaged in fleeting combat with state military forces throughout the Horn of Africa ... especially in the border region between Somaliland and Puntland;
8. Specific targets have included military units and bases of both host nations (HN) and UN/NATO contributing members, government offices and other symbols of authority, police units and security infrastructure, civil infrastructure, nongovernmental and international organizations' aid depots and distribution points, and transport. Development agency personnel, aid workers and their contractors, and shipping in the Gulf of Aden and western reaches of the Indian Ocean have also been targeted;

² Adapted from a Technical Memorandum developed for CFD (2010)

9. One of the greatest concerns is that radical Islamic/terrorist groups may use the lawless territories and chaotic political situation in Somalia as a transit area or staging ground for launching attacks throughout East Africa;
10. Despite the rise of a small, ruthless jihadist insurgency movement with greater ties to al-Qaeda or similarly inclined organizations in Somalia, the territory of Somaliland has remained relatively secure from the external influences of radical Islam. In Somaliland, the reliance on a system of clan and sub-clan elders has served as a moderating and peace-building force in managing the interaction between religion, custom and tradition, politics and modern secular nationalism. It is the pragmatic balance between competing forces that has allowed Somaliland to pre-empt and contain the more militant expressions of political Islam. Efforts by Islamic/terrorist groups to foment unrest, to this point, have not succeeded in igniting tensions with clan factions and business leaders, nor have they garnered broad support from the elites and population;
11. Considering the larger Somaliland business environment, international terrorist groups use the weak governance system in Somaliland to their advantage, operating front businesses to launder and generate funds to support activities. However, this activity is not widespread. While a vast majority of Somaliland businesses are legitimate, very small groups of committed radicals use businesses as a cover for buying weapons, operating safe havens and supporting the training of domestic insurgents in Puntland;
12. Two contested eastern border regions, the Sanaag and the Sool, lie at the heart of the conflict between Somaliland and Puntland ... The escalation of clan violence between Somaliland and Puntland over the disputed territories could pose a threat to Somaliland's internal stability. The tensions have periodically flared into armed clashes and border skirmishes between Somaliland security forces, Puntland forces and the local Dhulbahante militia. There is limited humanitarian activity, population displacement and restricted access due to the ongoing hostilities in the disputed region. The task of improving security continues to be made difficult by the wide availability of small arms and ammunition, and the numerous clan militias that can easily be mobilized. The security situation is exacerbated by overt and covert intervention of Ethiopia and Eritrea;
13. There is an absence of effective Somaliland control and administration throughout large parts of its own territory, particularly in the eastern regions;
14. Puntland efforts to enlist support for its clan-based militias in Somaliland from various Somali warlords is aimed at continuing the struggle to uproot the Sanaag and the Sool region through indirect means, largely in the form of providing support for piracy, terrorism, regional radicalism and criminal activity. The conflict represents a major challenge to state security institutions and law enforcement agencies ... Although AU peacekeeping forces in the disputed eastern regions have relied extensively on networks of clan leaders, who provide local intelligence and knowledge of the region, the challenge is ensuring they have enough resources to coordinate stabilization and reconstruction efforts with the rest of the coalition forces;
15. NATO ... Along with land force elements, most contributing members are also providing collective enablers such as aviation and maritime assets involved in intelligence, surveillance,

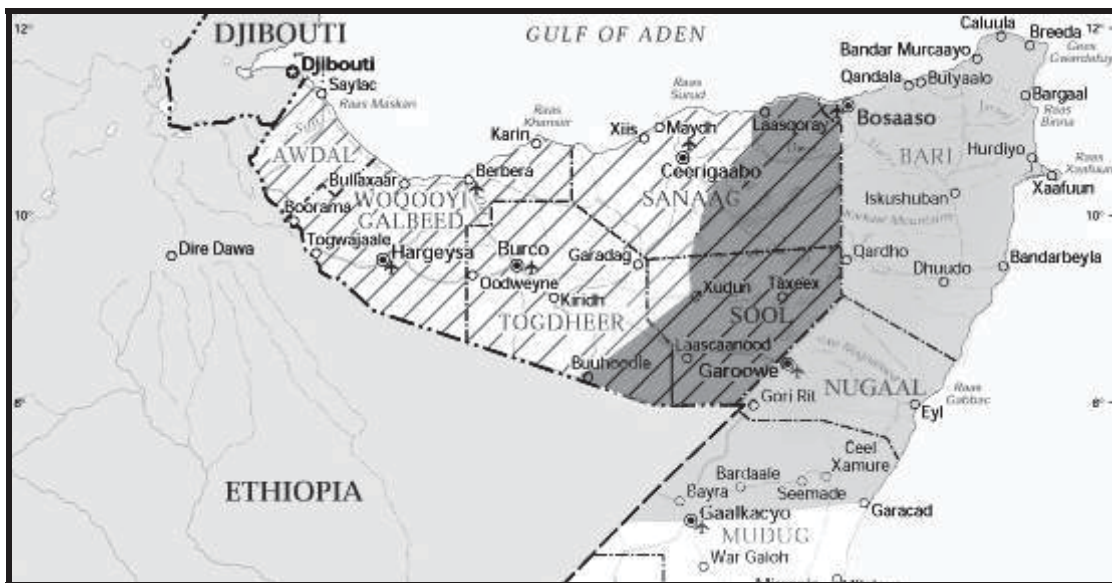
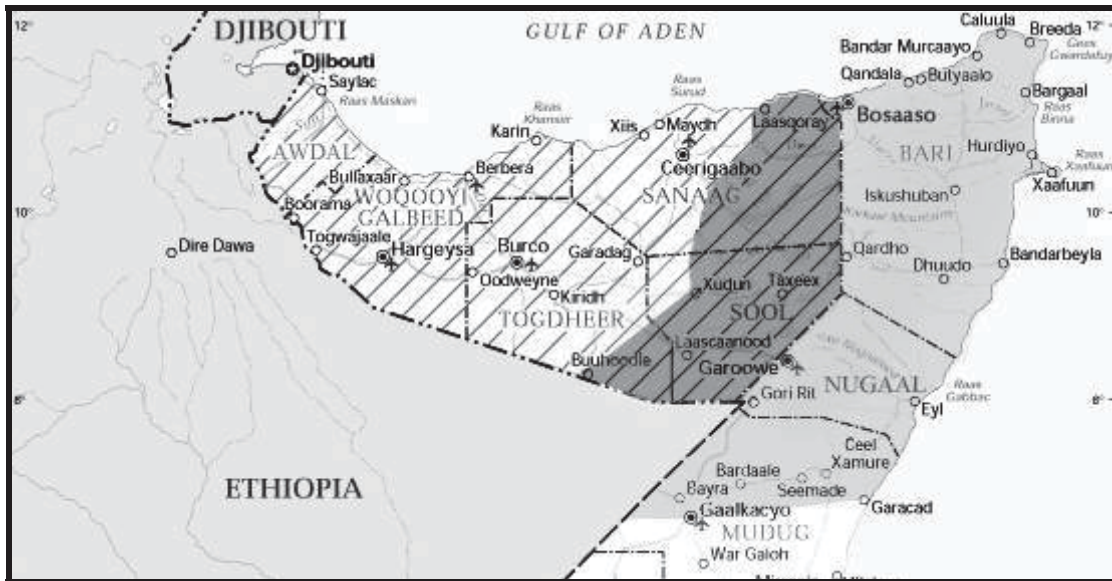
target acquisition and reconnaissance (ISTAR), C2 and other appropriate tasks. These assets include cyber-network and space-based elements;

16. Canada's mission: "Assisting development of national police forces, judicial system, and legal statutes; assisting development of national military forces; building new and strengthening existing government institutions; assisting in the delivery of core public services; assisting in the maintenance of the natural environment through sustainable urban and rural development; contributing to counter-terrorist activities; and, contributing to regional peace, security, and development";
17. The port of Berbera is Somaliland's sole deepwater anchorage. Located at the apex of the Addis Ababa – Hargeisa- Berbera and Hargeisa – Berbera – Burao transportation corridors, the port is critical to the Horn region's economic development;
18. Somaliland's military force is largely inexperienced and not capable of performing major combat or counter-insurgency operations;
19. The army is frequently tempted to impose its will over the contested region by force, but such actions could undermine support for recognition and draw forces in from elsewhere in Somalia or Puntland, ultimately fuelling separatist aspirations and becoming a source of long-term instability;
20. Somaliland possesses a domestic maritime police capacity ... coastguard is responsible for such operations as countering human trafficking, fisheries patrol anti-smuggling, search and rescue and environmental protection;
21. The Somaliland government continues to contract private security and military companies to strengthen the capability of local authorities. ... The private security companies are contracted primarily to improve security systems of the port in Berbera;
22. A military base in Djibouti serves as coalition headquarters with a full range of logistical, C2, and other support services. The base is co-located with the Djibouti Airport, where coalition strategic aviation assets are situated and is in close proximity to a seaport. Coalition naval ships use Djibouti's port facilities to support operations in and around the Gulf of Aden.
23. Full fibre-optic internet capability is available in country (two external links, one north to Djibouti and one off-shore through Berbera) in addition there is a wide-spread cell phone network throughout the country.

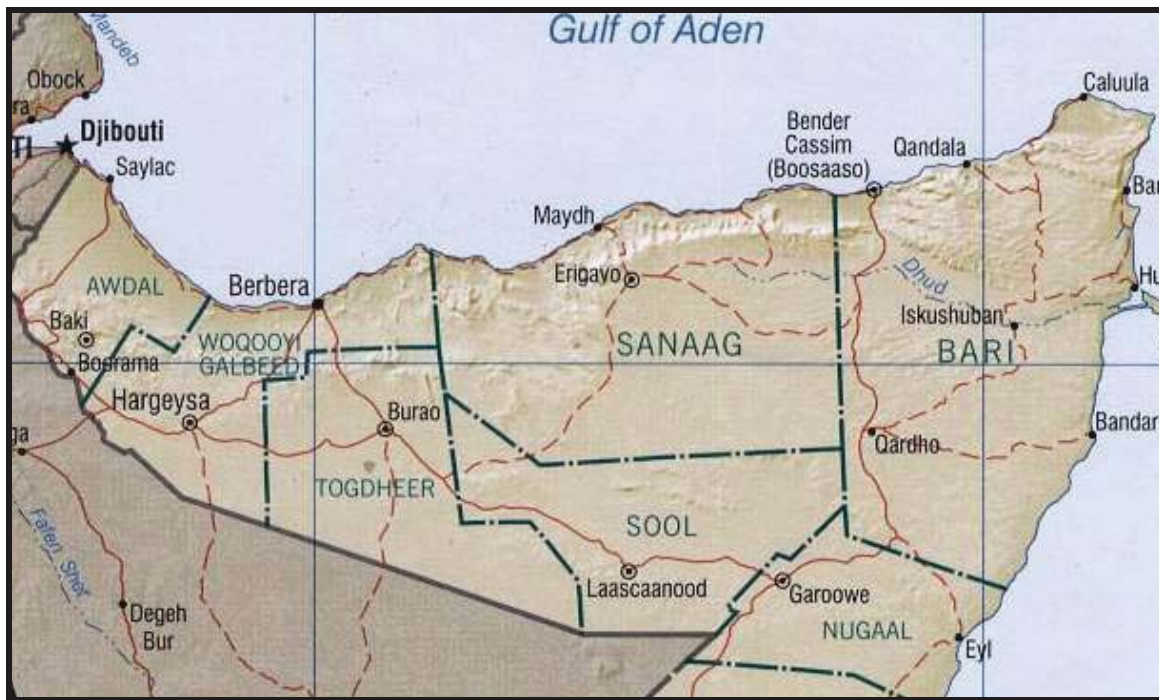
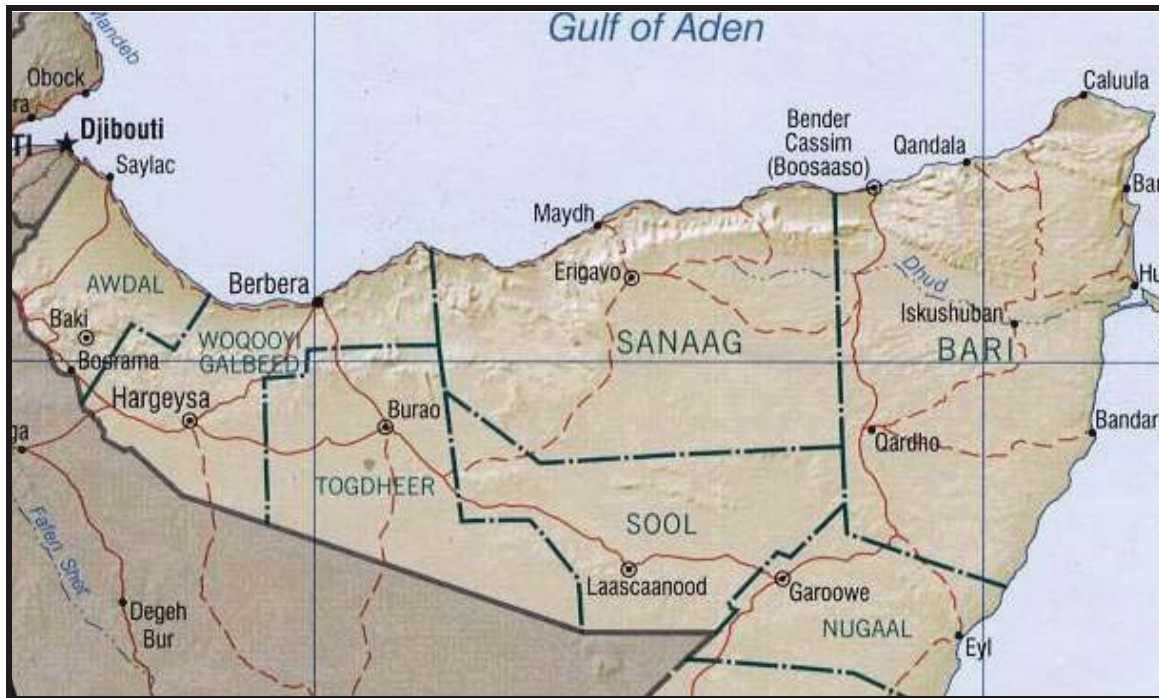
The following maps were given to the participants and were adapted on from:
http://www.lib.utexas.edu/maps/africa/somalia_rel02.jpg .



Somaliland and Puntland Political Regions and Disputed Territories



Relief Map of Somaliland and Northern Puntland



Annex C Sample IoS cards

V4P1-2

Methodology for Assessing Disruptions (MAD) Game

Idea of System: : Jolly Roger's Talking Parrot(s)

Land	X	Urban	X
Navy	X	Asymmetric	X
Air	X		

1. Description and Operational Interest

- Promotion of collaboration between forces by tracking RFID'd pirates (from previous technology)
- Foster cooperation and collaboration across forces and deny safe havens.

2. Performance range

- RFID tags 1000 nmi range need, construction of very large towers to monitor the 500 km range of the strait

3. Technologies incorporated

RFID, UAVs, tower or blimps for COMMS infrastructure, Network platform, Web 3.0

4. Likely maturity from 2020 onwards

10 year development likely in order to field a prototype

5. Countermoves to anticipated moves by the Red

Get counter Moves


- 1.
- 2.
- 3.

6. References

Contributors, articles, pictures, etc. that provide more detail on the technology

Additional Detail / Notes

- CONOPS
- 1. Tag denied pirates (from previous tech)
- 2. Predictive GIS technology to identify probable ports of call for Pirates
- 3. Use collaborative communication tool to allow partners to mount interdiction police operations



V5R-1

Methodology for Assessing Disruptions (MAD) Game

Idea of System: Banks are bad

Land	X	Urban	X
Navy	X	Asymmetric	X
Air	X		

1. Description and Operational Interest

Create regional economic instability;

- Cyber attack of the local banking system
- IO campaign on the instability of the banks – spray paint, social networking
- And we'll blow up some banks, too, since the paints will be the explosive type used in 9/11

2. Performance range

1

3. Technologies incorporated

Electronic potential for disruption if known or anticipated

4. Likely maturity from 2020 onwards

Electronic technology maturity level

5. Countermoves to anticipated moves by the Red

Get counter Moves


- 1.
- 2.
- 3.

6. References

Contributors, articles, pictures, etc. that provide more detail on the technology

Additional Detail / Notes

- Type of Weapon (e.g. Kinetic, Direct energy, Non-conventional) or sensor
- Impact on logistics, C4ISR, Mobility, Personnel protection, Influence etc.



Annex D Excerpts from the 26 feedback forms returned

Q1. Did MAD Part I enable the development of systems using PDT?

9 – Yes

7 – No

6 – Maybe

4 – N/A

Comments:

- May be too futuristic
- Need polishing
- Merge with other techs
- Inadequate time
- Concerned that time resulted in less complete than needed response
- Needs second iteration with OPP/COA

Q2. How would you run the MAD Part I differently?

Comments:

- Make defeat OPFOR part of objectives
- Lower number of vignettes (2 per day)
- Opportunity to prepare in advance
- Repeat this exercise in each lab
- OGD representative of whole of government
- More focused vignettes (to a single task or desired effect)
- Allow 5 minute group huddle prior to response
- Red team goes first provides its plan, then blue.
- Judge decide who has won initial contact, loser gets counter-move
- Story board development instead of IoS cards
- Do not change the rules mid-stream (in vignette or overall)
- Need to push the futuristic systems
- Counters need to be useful to the discussion meaning focused on the area of initial system in order to explore the system as opposed to complete military validation.

- Confrontation should be system, counter to system, etc. Each team presents their system and has the other team try to counter, in turn. (an example where this did happen, the denial of service bite-back, counter we will just use one of your computers “Goal is to build better cards”
- Put in the competitive arena is useful forum.
- No reason for adversarial confrontation
- No need for a winner
- More time required
- Did not find read-ahead package useful
- Facilitators
- Need note takers, white boards
- Trial run to help people can determine time pressures
- Problem if a vignette requires a specific knowledge
- Add an actual adversary in vignette (PRC/PLA) ie equivalent
- All vignettes in read ahead
- Facilitators to handle group dynamics, authority to ensure all get a chance to talk
- Run vignettes multiple times rather than once.
- Operational relevance validation as well as potential for disruption validation.
- Vignettes did not provide for some types of technologies
- Need more time in confrontation phase
- Reference and pictures not used in time
- Don’t like powerpoint – remove countermoves from IoS template
- No time for references etc.
- Add more detail (ORBAT) in vignettes

Q3. How would you suggest that IoS cards are developed in the future and who should develop them?

Comments

- IoS creation prior to arrival
- Team should have CF operator-CF engineer-DS
- Done in unit/section/group
- Could use confrontation to assess previously developed cards
- By technical SME

- Different forum, but use confrontation to lead to part II
- SME in lab for initial input
- Where to put aim/mission/task on IoS card
- Purple + red = one card

General comments

- No powerpoint
- Takes time to develop team
- Use existing teams in labs with current format
- Much smoother in day 2
- Need objectives to be more focused
- Red-blue objectives should be opposite
- Did not address merging nature of disruptive technologies
- Take list of high-readiness technologies, and medium readiness technologies
- Brainstorming did not reach disruptive
- Development of technologies takes time, changing policy takes longer
- Consideration of constraints etc. – support free-play to brainstorm
- Better over a week then 2 days
- Seek to learn and observe from other countries
- Computer-based game
- Need more computers to access the internet
- Spot for undeveloped ideas
- Cannot get speed, quality, quantity at same time
- Does not like adversarial
- Need for material in different forms, computer, paper ...
- Not enough time to consider background material (walls..
- Purple vs. purple competition not required.
- Confrontation good
- Need to talk about PDT concept – merger of technologies
- Vignette should lend itself to particular technical solution – counter-insurgency focuses people on low-tech solutions
- Set capability of adversaries

List of abbreviations

ADM	Assistant Deputy Minister
AI	Artificial Intelligence
AU	African Union
C2	Command and control
CBR	Chemical Biological and Radiological
CDI	Chief Defence Intelligence
CF	Canadian Forces
CFD	Chief of Force Development
CL	Convening Letter
COA	Courses of Action
COS (S&T)	Chief of Staff (ADM (S&T))
CS Net	Chief Scientists' Network
DTAG	Disruptive Technologies Assessment Game
EMP	Electro Magnetic Pulses
FPG	Functional Planning Guidance
GoC	Government of Canada
IoS	Idea of System card
ISTAR	Intelligence, Surveillance Target Acquisition and Reconnaissance
J&I	Judgments and Insights
MAD	Methodology for Assessing Disruptions
NATO	North Atlantic Treaty Organization
NGO	Non -Governmental Organization
NUNHOA	NATO/United Nations Mission Horn of Africa
OCS	Office of Chief Scientist
PDT	Potentially Disruptive Technology (ies)
QRF	Quick Reaction Force
SA	Situational Awareness
SE	Synthetic Environment
TDP	Technology Demonstration Project
TIF	Technology Investment Funds

UAV	Unmanned Air Vehicles
UN	United Nations

This page intentionally left blank.

Distribution list

Document No.: DRDC Corporate TM 2012-009

LIST PART 1: Internal Distribution by Centre

Pierre Lavoie, DRDC Corporate
Gitanjali Adlakha-Hutcheon, DRDC Corporate

Paul Hubbard, DRDC Ottawa

Scott McLelland, DRDC Ottawa
Mike Vinnins, DRDC Ottawa
Bill Katsube, DRDC Ottawa
Chris McMillan, DRDC Ottawa

Mark Hazen, DRDC Atlantic
Francine Desharnais, DRDC Atlantic
Calvin Hyatt, DRDC Atlantic
DRDC Atlantic Library

Kevin Sprague, DRDC CORA

<rest of CS Net>

0 TOTAL LIST PART 1

LIST PART 2: External Distribution by DRDKIM

1 Library and Archives Canada

1

 TOTAL LIST PART 2

0 TOTAL COPIES REQUIRED

This page intentionally left blank.

DOCUMENT CONTROL DATA		
(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)		
1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.) Defence R&D Canada305 Rideau Street Ottawa, Ontario K1A 0K2	2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.) (Non-controlled goods) DMC A Review:GCEC June 2010	
3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.) Methodology for Assessing Disruptions (MAD) Game Part I: Report and Analysis		
4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used) Adlakha-Hutcheon G., Hazen M., Hubbard P., McLelland S., Sprague K.		
5. DATE OF PUBLICATION (Month and year of publication of document.) December 2012	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.) 62	6b. NO. OF REFS (Total cited in document.) 11
7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.) Technical Memorandum		
8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.) Defence R&D Canada305 Rideau Street Ottawa, Ontario K1A 0K2		
9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)	
10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.) DRDC Corporate TM 2012-009	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)	
11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.) Unlimited		
12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.) Unlimited		

13. **ABSTRACT** (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

The memorandum reports on the Methodology for Assessing Disruptions (MAD) game played at DRDC Ottawa on 5-6 October 2010. This event was Part I of a two-part seminar wargame. In Part I, scientists and CF members participated in a two-step brainstorming and red-teaming process to develop futuristic ideas of systems that may provide an operational advantage to the CF. A total of 47 idea of system cards were produced in Part I. These will be assessed for their disruptive potential through a series of wargames in Part II, which will take place in January, 2011. Feedback solicited through a Judgments and Insights session and formal feedback forms brought to light several ideas for improving the gaming methodology for future iterations of MAD. The game was successful in fostering innovation through confrontation-based red-teaming as well as socializing potentially disruptive technologies elaborated in the ADM (S&T) Functional Planning Guidance. This memorandum is intended primarily for the Office of the Chief Scientist (OCS) DRDC and the Chief Scientists Network (CSNet). It will also be of interest to others in the S&T community within DRDC and its CF partner organizations such as the Chief Force Development and the environmental warfare centres.

Le mémorandum technique traite du jeu MAD (méthodologie d'évaluation des perturbations) joué à RDDC Ottawa les 5 et 6 octobre 2010. Cet événement fut la première partie d'un exercice de jeu de guerre en deux composantes. Dans la première partie, des scientifiques et des membres des FC ont participé à un processus en deux étapes de remue-ménages avec équipes rouges dans le but d'élaborer des idées de systèmes futuristes susceptibles de fournir un avantage opérationnel aux FC. Au total, 47 cartes d'idées de systèmes ont été réalisées au cours de la première partie. Celles-ci seront évaluées pour leur potentiel perturbateur dans le cadre d'une série de jeux de guerre lors de la deuxième partie qui aura lieu en janvier 2011. La rétroaction sollicitée par l'entremise d'une séance de jugements et d'idées ainsi que de formulaires de rétroaction formelle ont mis en lumière plusieurs idées permettant d'améliorer la méthodologie des jeux pour les versions futures des jeux MAD. Le jeu a permis de favoriser l'innovation grâce à l'utilisation d'équipes rouges fondée sur la confrontation de même qu'à la socialisation de technologies potentiellement perturbatrices élaborées dans le Guide de planification fonctionnelle du groupe du SMA(S&T). Le présent mémorandum technique est principalement destiné au Bureau du scientifique en chef (BSC) de RDDC et au Réseau des scientifiques en chef (CSNet). Elle pourra également intéresser d'autres intervenants de la collectivité des S & T au sein de RDDC et des organisations partenaires des FC, notamment le Chef du Développement des Forces et les centres de guerres environnementales.

14. **KEYWORDS, DESCRIPTORS or IDENTIFIERS** (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Potentially Disruptive Technology, PDT, Idea of Systems, IoS, Disruptive Technology Assessment Game, DTAG, Methodology for Assessing Disruptions, MAD, red-teaming, wargame, confrontation, R&D priorities, functional guidance

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale



www.drdc-rddc.gc.ca